Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matters of

9-1-1 Governance and Accountability	PS Docket No. 14-193
Improving 911 Reliability	PS Docket No. 13-75

COMMENTS OF THE
VIRGINIA STATE CORPORATION COMMISSION

Introduction

The Division of Communications of the Virginia State Corporation Commission ("VSCC Staff") respectfully submits these comments in response to the Federal Communications Commission's ("FCC") Policy Statement and Notice of Proposed Rulemaking ("Notice") released on November 21, 2014 in PS Docket Nos. 14-193 and 13-75.[1] The Notice proposes "specific rules designed to address failures leading to recent multi-state 911 outages, based on the October 2014 report of the Public Safety and Homeland Security Bureau."[2]

Discussion

The Notice highlights the continuing importance of ensuring 911 reliability to the nation as we transition from the legacy 911 Time Division Multiplexing networks to an Internet Protocol ("IP")-based Next Generation 911 ("NG911") architecture. The Notice states:

> While legacy 911 infrastructure remains in use throughout much of the country, recent events have shown that evolving technology, while providing many

[1] The VSCC Staff submitted comments in PS Docket Nos. 13-75 and 11-60 on May 13, 2013.

[2] Notice, para. 4.

> benefits to PSAPS and the public, also has introduced new and different risks. A growing number of disruptions to 911 service are caused by software malfunctions, database failures, and errors in conversion from legacy to IP-based network protocols.[3]

As the FCC is aware, Northern Virginia experienced a major 911 outage following the June 2012 Derecho. That outage primarily involved Verizon's legacy 911 network. The VSCC opened a proceeding requiring its staff to conduct an investigation into that outage.[4] To date, we have issued three reports detailing the event, root causes, and recommendations.[5] Most recently, we issued a status report detailing the progress Verizon has made in addressing the weaknesses found in its procedures, processes, and central offices.[6] This status report, at pages 7 through 13, also discusses the FCC's December 12, 2013 Report and Order in PS Docket Nos. 13-75 and 11-60; and, at pages 13 through 15, identifies several concerns with the 911 rules adopted by the FCC in that proceeding. In addition, this status report recommends modifying some of the current requirements for Verizon in light of the progress that has been made to date. It also adds two recommendations relating to the FCC's 911 outage reporting and 911 service provider certification requirements as follows:

- Verizon should provide the Staff with the Initial and Final Communications Outage Reports required pursuant to 47 C.F.R. Part 4 for outages impacting 911

[3] Notice, para. 20.

[4] *Commonwealth of Virginia, ex rel. State Corporation Commission, Ex Parte: In the matter of investigating 911 emergency call service outages and problems,* Case No. PUC-2012-00042, 2012 S.C.C. Ann. Rep. 200, Order Establishing Investigation, (July 3, 2012).

[5] Case No. PUC-2012-00042. Reports filed on September 14, 2012, January 17, 2013, and December 31, 2014.

[6] A copy of the December 31, 2014 VSCC Staff Status Report in Case No. PUC-2012-00042 is attached to these comments.

service in Virginia. When providing such reports, Verizon should comply with all provisions of the FCC regulations related to report content, processing, and delivery. Upon request, Verizon should provide the Staff with additional information regarding a reported 911 service outage in Virginia that may not be included in the FCC report.[7]

- Verizon should provide the Staff with copies of all applicable portions of the initial (October 15, 2015) and first full (October 15, 2016) annual certification reports filed with the FCC pursuant to 47 C.F.R. § 12.4, including any protected confidential information, that impact the reliability of 911 service (i.e. circuit auditing, backup power, and network monitoring) in Virginia.[8]

In Virginia, pursuant to § 56-484.14 (3) of the Code of Virginia, the E-911 Services Board has the duty to:

> Develop a comprehensive, statewide enhanced 9-1-1 plan for wireless E-911, VoIP E-911, and any other future communications technologies accessing E-911 for emergency purposes. In constructing and periodically updating this plan as appropriate, the Board shall monitor trends and advances in enhanced wireless, VoIP, and other emergency telecommunications technologies, plan and forecast future needs for these enhanced technologies, and formulate strategies for the efficient and effective delivery of enhanced 9-1-1 services in the future with the exclusion of traditional circuit-switched wireline 9-1-1 service.

On March 8, 2012, "Virginia's Next Generation 9-1-1 Implementation Plan" was presented to the E-911 Services Board. In addition, the E-911 Services Board recently commissioned an IP-Based 911 Network Feasibility Study, and a final report was submitted to the Virginia Information Technologies Agency in January of 2015. Virginia is addressing the transition to NG911 as various localities (PSAPs) are making progress

[7] Case No. PUC-2012-00042, December 31 2014 VSCC Staff Status Report, p. 19

[8] Ibid.

with implementing more advanced applications and infrastructure. However, Virginia still relies heavily on the legacy 911 networks in ensuring the public safety of its citizens.

We support the FCC's efforts to ensure the safety of our citizens during (and after) the transition to an NG911 architecture. It is important to recognize that while this transition will bring many benefits, it brings new risks and challenges, as the FCC has recently learned. The VSCC Staff stated in previously submitted comments that:

> it is unlikely that a set of regulations could be sufficiently detailed to address all the necessary operational parameters and situations. We believe that balance will best be achieved by focusing efforts on identifying public safety needs and preventing potentially life threatening events. Finding a carrier to be in noncompliance with a rule or regulation can generally be an effective tool for regulators, but in the public safety arena the priority must be on prevention versus determining blame after a tragic event.[9]

The FCC and appropriate state and local authorities must continue to collaborate and work together to achieve our joint objective of ensuring the public's safety. The Notice recognizes that an IP-based 911 network architecture is bringing new providers and vendors into the marketplace and therefore increasing the risk of a 911 outage impacting multiple states. Nonetheless, the FCC should be careful in crafting its NG911 regulations to not interfere with states' statutory or regulatory authority to manage jurisdictional 911 emergency services. As the Notice recognizes, "many decisions regarding 911 deployment, operations, and cost recovery are best made at the state and local level, and continued oversight by states and localities is vital to ensuring that 911 service remains effective and reliable in every community across the country."[10]

[9] May 13, 2013 VSCC Staff comments filed in PS Docket Nos. 13-75 and 11-60, pp. 7-8.

[10] Notice, para. 38.

The Notice points out that "the increasing complexity of IP-based 911 network architecture, combined with the increased diversity of entities supporting 911 capabilities, creates potential obstacles to establishing prompt situational awareness and initiating recovery from major 911 outages."[11] Situational awareness and coordination are key components in mitigating the impact of any 911 outages even in the 911 legacy network. We share the FCC's goal of improving this awareness and coordination particularly as we transition to NG911 networks. As part of this effort, the FCC should ensure that state commissions and other relevant state agencies have timely access to any 911 outage notification and information provided to the FCC.

Conclusion

NG911 will offer advanced features and functions that will benefit consumers and the public safety community. However, as the Notice recognizes, we need to be vigilant in ensuring that public safety is not jeopardized as we transition to an IP-based 911 architecture. We encourage and support the FCC's efforts in this proceeding to ensure the continued reliability of 911 to all citizens in Virginia and the nation.

Respectfully submitted,
Virginia State Corporation Commission Staff

William Irby
Director
Division of Communications

March 23, 2015

[11] Notice, para. 64.

141123 0097

COMMONWEALTH OF VIRGINIA

SCC-CLERK'S OFFICE
DOCUMENT CONTROL CENTER

STATE CORPORATION COMMISSION

2014 DEC 31 P 3:08

STAFF
STATUS REPORT

DIVISION OF COMMUNICATIONS

CASE NO. PUC-2012-00042

IN THE MATTER OF
INVESTIGATING 911 EMERGENCY
CALL SERVICE OUTAGES AND PROBLEMS

December 31, 2014

1412290697

TABLE OF CONTENTS

1412360057

INTRODUCTION

After receiving reports of 911 emergency call service outages and problems following the storms that struck parts of the Commonwealth[1] in June of 2012, the Commission issued an Order Establishing Investigation ("July 3, 2012 Order") directing its Staff ("Staff") to investigate the loss of 911 emergency call services from the June storms. The focus of the investigation was on the outages and problems following a massive derecho that occurred on June 29, 2012 ("June 29 Derecho"). The July 3, 2012 Order required the Staff to report its preliminary findings by September 14, 2012, and to file a report with its final findings and recommendations by December 31, 2012. At the Staff's request, the date for filing this report was extended to January 17, 2013.

The report of the Staff's preliminary findings ("Preliminary Findings Report") was filed on September 14, 2012, and the report of the Staff's final findings and recommendations ("Final Report") was filed on January 17, 2013.

On February 22, 2013, the Commission issued an Order ("February 22, 2013 Order") concurring with the recommendations of the Staff[2] contained in its Final Report. Two of those were:

- The Staff should file an annual status report with the Commission that includes recommendations on continuing the various requirements on Verizon and/or recommendations on any changes or additions to such.

---

[1] Northern Virginia was the most significantly impacted area.

[2] In the February 22, 2013 Order, the Commission stated: "We find the recommendations listed in the Staff's Final Report are reasonable, responsive to our order initiating this investigation, and should continue to be implemented by Verizon and the Staff forthwith. In addition, we agree with the Staff that this docket should remain open to monitor and facilitate the implementation of such recommendations, including but not limited to, the receipt of the reports referenced therein."

- The Staff should evaluate the FCC Public Safety and Homeland Security Bureau's Report and Recommendations released on January 10, 2013, and advise the Commission of any additional recommendations we may determine are warranted based on that report.

On December 12, 2013, the Federal Communications Commission ("FCC") issued a Report and Order ("Report and Order") in PS Docket Nos. 13-75 and 11-60.[3] The Report and Order adopted rules to improve the reliability and resiliency of 911 communications networks nationwide. The FCC recognized that millions of Americans were without 911 services for a period of time as a result of the June 29 Derecho. "After a comprehensive inquiry into the causes of 911 outages during the derecho, as well as 911 network reliability more generally, the Public Safety and Homeland Security Bureau (PSHSB or Bureau) determined that many of these failures could have been mitigated or avoided entirely through implementation of network-reliability best practices and other sound engineering principles."[4]

The purpose of this report is to satisfy the above items from the Commission's February 22, 2013 Order. However, as the FCC has acted on the PSHSB Report and Recommendations, we instead evaluate the FCC's Report and Order. We also discuss Verizon's compliance with its overall corrective action plan and the recommendations in the February 22, 2013 Order.

---

[3] In the Matter of Improving 911 Reliability and Resiliency; and Continuity of Communications Networks, Including Broadband Technologies. Order may be found at http://www.fcc.gov/document/fcc-adopts-rules-improve-911-reliability

[4] Report and Order, para. 2.

1417903677

DISCUSSION

In this section, we discuss the status of Verizon's compliance with the recommendations in the February 22, 2013 Order. In addition, we describe the Staff's ongoing monitoring and inspection efforts since filing our Final Report.

Status of Verizon Compliance

We are pleased that Verizon has made significant progress in implementing the recommendations set forth in our Final Report. To date, Verizon has filed seven quarterly corrective action progress reports with the Commission.[5] In addition, the Staff has held quarterly meetings with Verizon to discuss the progress on corrective actions, audits, inspections, and other initiatives for each of the seven quarters (1Q 2013, 2Q 2013, 3Q 2013, 4Q 2013, 1Q 2014, 2Q 2014, and 3Q 2014) since the February 22, 2013 Order. As the corrective action progress reports show, Verizon has been complying with the recommendations of our Final Report. While numerous deficiencies (with differing degrees of severity and safety) have been found through the various audits and inspections, Verizon has made substantial progress in correcting the deficiencies. There were over two hundred recommendations from the initial power audits in the 16 mission critical offices and all items were remediated.[6]

[5] Filed on May 7, 2013, July 25, 2013, December 2, 2013, February 11, 2014, June 6, 2014, July 29, 2014, and December 1, 2014.

[6] The Verizon 1Q 2014 Corrective Action Progress Report, (p. 3) shows all items completed for the 16 mission critical offices.

4123093

In addition, during 2013, Verizon completed the audit work in all remaining Virginia offices.[7] We have received copies of all the additional audits required by the February 22, 2013 Order. According to Verizon's 3Q 2014 progress report, it has identified nearly 4000 action items from the 2013 power audits and other ongoing inspection programs. Verizon continues to prioritize remediation on the most critical items first. We note that many of these deficiencies are being found and corrected through Verizon's annual Clean, Neat, Safe and Reliable program.[8] In addition, Verizon completed battery inspections and testing in its Virginia offices by 2Q 2013 and again in the second half of 2013 for compliance with its semi-annual battery maintenance program.[9] Furthermore, according to the 3Q 2014 progress report, Verizon is on track to complete its semi-annual battery maintenance compliance for 2014.

Verizon has also made significant progress inventorying its 911 service infrastructure and has completed diversity reviews for all Verizon-served PSAPs in Virginia. Remediation has been completed for most PSAPs and the remaining ones are partially complete or scheduled for remediation. The VLSS (Verizon Lean Six Sigma) Project is being used to improve Verizon's processes for determining the availability and sufficiency of spare parts for manufacturer discontinued equipment (i.e., rectifiers). The discontinued equipment procedures and instructions have been revamped to ensure technicians are able to obtain replacement rectifiers and cards in a more expeditious fashion.

---

[7] Verizon conducted a total of 307 additional audits in Virginia in 2013 (for a total of 323 audits including the original 16).

[8] Verizon inspected over 200 offices in Virginia in 2013 and almost 300 offices in 2014 as part of this program. More than 1500 items were identified in the 2014 inspections.

[9] This program covers all central offices and associated remotes.

4902521

Staff Monitoring Role

One of the recommendations in the Final Report was for Verizon to permit the Staff to monitor any audit as it was conducted. Verizon provided the Staff with its schedules for such audits and readily accommodated our interest and availability. We accompanied Verizon personnel during power audits in several central offices.[10] We found Verizon to be strongly committed to the audit process and we are pleased with the speed in which it has undertaken these audits. Overall, we have been impressed with the thoroughness, professionalism, and expertise of all the individuals conducting and involved with the audits.

Our current focus is ensuring that all deficiencies and recommendations identified in the power audits are corrected properly and as quickly as possible. We have revisited the 16 mission critical offices where Verizon's initial power audits were conducted in 2012 to inspect their overall current condition. The 1Q 2014 corrective action progress report shows that all deficiencies from the initial power audits have been fully completed in those 16 offices.[11] Verizon's remediation efforts were evident in these revisits.

The major 911 outage problems resulting from the June 29 Derecho originated from the failed generator starts at the Arlington central office. Therefore, the Arlington office was the first to be re-inspected (in October 2013). The improvements and overall cleanliness in this office (as compared to our earlier visit shortly after the June 29 Derecho) were striking. Not only had Verizon corrected all the deficiencies identified in the audit for this office, it was apparent that the Verizon personnel were extremely proud

[10] The Staff also saw several audits conducted under Verizon's Clean, Neat, Safe and Reliable program.

[11] Note: We expect this to be shown as completed in the 1Q 2014 report.

1412290897

of their efforts.

Overall, all 16 mission critical offices were found to be in good condition. We found the generators and other power equipment to be in working order and properly maintained. Generally, only minor issues were seen (if any) with the most significant concerns being hot spots found in several offices, and one office where a roof leak was still apparent.[12]

Other Local Exchange Carriers ("LECs")

The Preliminary Findings Report noted that Verizon was the only LEC in Virginia that experienced significant 911 service problems following the June 29 Derecho, which primarily impacted Verizon territory. Nonetheless, we sought additional information regarding the preparedness of the other LECs in Virginia. Specifically, we sent letters to all the other incumbent local exchange carriers ("ILECs") requesting data regarding 911 services provided to PSAPs, backup power arrangements, and maintenance practices in their central offices. In addition, we performed visual walk-through inspections at various ILEC central offices.[13]

Overall, we found the other ILECs' offices to be in very good condition with proper (and routine) maintenance procedures being followed. In a few instances, we pointed out relatively minor issues to ILEC personnel during the inspections (that were easily corrected), and we did not find any situations that warranted further specific corrective action plans or necessary follow-up.

---

[12] Verizon was using fans to cool down these hot spots and has scheduled a roof replacement.

[13] We visited a representative cross section of offices, encompassing most of ILECs in the state (CenturyLink, TDS, MGW, Lumos, Shentel, Frontier, and Fairpoint). We did not inspect any of the telephone cooperatives' offices.

1413097

On April 1, 2014, the Staff met with Cox Communications at its Norfolk office to discuss its 911 preparedness. That meeting included a visual tour of its 5E switch, and in particular, the backup power sources (generators and batteries) at that office. We were impressed with the cleanliness, security, and overall condition of the equipment. No corrective action plan or further follow-up was necessary.

One of the other Staff recommendations found to be reasonable in the February 22, 2013 Order was for the Staff to continue to communicate and meet with the PSAP community. We have done so, and as part of such communication, the Metropolitan Washington Council of Governments 911 Director's Committee has advised that it would like for the recommendations dealing with PSAPs (the one above as well as the one saying Verizon should continue to meet and cooperate with PSAPs) should remain in effect.

FCC REPORT AND ORDER

In its report, the FCC determined that a purely voluntary best practices policy had not been adequate for ensuring 911 reliability. Accordingly, it adopted annual certification rules[14] to apply to every "Covered 911 Service Provider" as defined by the FCC. A Covered 911 Service Provider is defined as:

> any entity that provides 911, E911, or NG911 capabilities such as call routing, ALI, ANI, or the functional equivalent of those capabilities, directly to a PSAP, statewide default answering point, or appropriate local emergency authority, or that operates one or more central offices that directly serve a PSAP. For purposes of these rules, a central office "directly serves a PSAP" if it (1) hosts a selective router or ALI/ANI database (2) provides functionally equivalent NG911 capabilities, or (3) is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. This definition encompasses entities that provide capabilities to route 911 calls and associated

[14] The FCC's revised rules are attached to this report as Attachment 1.

14230097

data such as ALI and ANI to the appropriate PSAP, but *not entities that merely provide the capability for customers to originate 911 calls.*[15]

The Report and Order requires "that Covered 911 Service Providers (1) take reasonable measures to ensure reliable 911 service and (2) certify annually that they do so by adhering either to specified, essential practices based on established industry consensus or to appropriate alternative measures demonstrated to be reasonably sufficient to mitigate the risk of failure."[16] The FCC rules regarding the necessary reasonable measures are intended "to ensure 911 circuit diversity, availability of backup power at central offices that directly serve PSAPs, and diversity of network monitoring links (the "reasonable measures" requirement)."[17]

Covered 911 Service Providers will be required to demonstrate they have performed all the required reasonable measures to provide reliable 911 service through the certification process, but are not required to file support documentation. However, the support documentation must be retained for two years and be made available to the FCC upon request. The certification filing will "be deemed to satisfy the obligation to take reasonable measures to provide reliable 911 service, provided that the certification is accurate and complete."[18]

If a Covered 911 Service Provider cannot certify affirmatively to every element required for the annual certification, it may certify that it has taken reasonable alternatives measures. In any such circumstances, the Covered 911 Service Provider

---

[15] Report and Order, para. 36.

[16] Ibid, para. 44.

[17] Ibid, para. 45.

[18] Ibid, para. 48.

must include an explanation with its certification for each alternative why those alternative measures are reasonable.[19] The annual certification filing requirement does not take effect until two years from the effective date of the new FCC rules. According to the Report and Order, one year after the effective date of the new rules, Covered 911 Service Providers are required "to file an initial certification that they have made substantial progress toward meeting the standard of the full certification."[20]

On November 18, 2014, the PSHSB issued a public notice announcing that the effective date of the certification rules was October 15, 2014. The initial certification will be due to the FCC on October 15, 2015, and the first full annual certification will be due October 15, 2016.

911 Circuit Diversity Certification

> Covered 911 Service Providers must certify annually whether they have, within the past year, audited the physical diversity of critical 911 circuits or equivalent data paths to each PSAP they serve, tagged those circuits to minimize the risk that they will be reconfigured at some future date, and eliminated all single points of failure between the selective router, ALI/ANI database, or equivalent NG911 component, and the central office serving each PSAP.[21]

Alternatively, in lieu of eliminating all single points of failure, a Covered 911 Service Provider may certify that sufficient measures have been taken to mitigate the risk of the lack of physical diversity.[22] The FCC is requiring providers to conduct annual 911 circuit diversity audits, but providers "may take a range of corrective measures most appropriate

---

[19] Ibid, para. 62. Such alternative measures certifications are subject to more detailed review by the PSHSB.

[20] Ibid, para. 65. Substantial progress is defined as at least 50 percent compliance with each of the three substantive certification requirements.

[21] Ibid, para. 80.

[22] Another alternative is that a provider may certify why it believes this element of the requirements is not applicable to its network.

14139097

for their networks and PSAP customers."[23]

Central Office Backup Power Certification

> Covered 911 Service Providers are required:
>
> to certify annually whether they have sufficient, reliable backup power in any central office that directly serves a PSAP to maintain full service functionality, including network monitoring capabilities, for at least 24 hours at full office load. Further, we require the especially critical central offices that host selective routers to be equipped with at least 72 hours of backup power at full office load. The specified level of backup power may be provided through fixed generators, portable generators, batteries, fuel cells, or a combination of those or other such sources so long as it meets the applicable certification standard.[24]

If that level of backup power is not feasible in a specific central office, the Covered 911 Service Provider must state why in its annual certification and describe the alternative measures it has taken to mitigate the risk of not adhering to the required backup power configurations. The Report and Order recognizes that different central offices can present different backup power challenges and does not require a single solution. The rules allow "911 service providers flexibility to maintain adequate central-office backup power based on best practices and reasonable alternatives to suit site-specific circumstances."[25]

The FCC's backup power requirements are not applicable to all central offices but rather only to those "that could create choke points between the Covered 911 Service Provider networks and PSAPs."[26] Moreover, the FCC has adopted a dual standard requirement where 72 hours of backup power is applied to those central offices that host

---

[23] Report and Order, para. 80.

[24] Ibid, para. 107.

[25] Ibid, para. 109.

[26] Ibid, para. 114.

74253057

selective routers "because the failure of one selective router could disrupt service to an entire region and prevent re-routing of 911 calls to other PSAPs...."[27] On the other hand, only 24-hour backup power is required at all other central offices directly serving PSAPs. The Report and Order does not adopt specific backup power testing standards (i.e., full load testing), but Covered 911 Service Providers are required, "consistent with CSRIC[28] best practice, to certify that they test their backup power equipment according to the relevant manufacturers' specifications."[29] The Report and Order recognizes "that interdependent tandem generators were a primary cause of the failure of Verizon's central office power backup during the June 2012 derecho."[30]

However, the FCC rules do not specifically require that tandem generators be electronically separated. Instead, the rules require that a 911 provider certify whether it employs stand-alone backup power sources. In the alternative, they allow Covered 911 Service Providers "an opportunity to demonstrate that alternative measures upon which they rely (e.g., load shedding) are reasonably sufficient to mitigate the risk of failure."[31]

Network Monitoring Certification

Covered 911 Service Providers are required:

---

[27] Ibid

[28] Communications, Security, Reliability, and Interoperability Council.

[29] Ibid, para. 117.

[30] Ibid, para. 118.

[31] Ibid

> to certify annually whether they have, within the past year: (1) audited the physical diversity of the aggregation points that they use to gather network monitoring data in each 911 service area and the network monitoring links between such aggregation points and their NOC(s);[32] and (2) implemented physically diverse aggregation points for network monitoring data in each 911 service area and physically diverse links from such aggregation points to at least one NOC or, in light of the required audits, taken specific alternative measures reasonably sufficient to mitigate the risk of insufficient physical diversity.[33]

The FCC emphasizes that accurate situational awareness (i.e., network monitoring) is extremely important during a network outage. For example, the Report and Order points out that two primary 911 service providers lost network monitoring capabilities during the 2012 Derecho and "in both instances a widespread loss of network monitoring capabilities could be attributed to a single point of failure, such as one central office collecting telemetry data for dozens of facilities in northern Virginia."[34]

The FCC recognizes that complete physical diversity is likely not achievable in all circumstances and allows service providers "with the flexibility to compensate for an inability to conform to our certification standard by employing appropriate alternative measures...."[35] In addition, a Covered 911 Service Provider may certify that (and explain why) complete physical diversity may not be feasible to its network.

PSAP Outage Notification

In addition to the certification requirements discussed above, the Report and Order amended the rule regarding notification of 911 outages to PSAPs. Under the amended rule, "Covered 911 Service Providers must notify PSAPs of outages potentially

---

[32] Network Operations Center ("NOC")

[33] Ibid, para. 131.

[34] Ibid, para. 133.

[35] Ibid, para. 137.

14123697

affecting 911 service to that PSAP within thirty minutes of discovering the outage and provide contact information such as name, telephone number, and e-mail for follow-up."[36] The prior rule only required the service provider to notify PSAPs "as soon as possible." In addition, Covered 911 Service Providers must communicate additional, more detailed information to PSAPs, including estimated time of repair, no later than two hours after the initial communications.

Concerns with FCC Report and Order

Overall, we applaud the FCC's new rules as a significant improvement over the previous voluntary best practices policy. We expect these rules to have a major impact on LEC readiness with respect to the reliability and resiliency of their 911 communications networks. Nonetheless, we have some concerns with the FCC's rules regarding this Commission's ability to rely fully on those rules to meet the specific needs of the Commonwealth. We support an annual certification process as it would be nearly impossible to develop rules in sufficient detail to address all necessary 911 requirements. However, there are limitations to relying on certification filings, and we identify several possible areas of concern as follows:

- Covered 911 Service Providers are not required to comply fully with all certification requirements until October 2016. This may be a reasonable timeframe to allow the providers sufficient time to implement all the necessary network requirements. However, associated risks to 911 communications may remain or develop with incomplete compliance during the next two years.
- Relying on certification and attestation filings without requiring more detailed

[36] Ibid, para. 140.

1496214

supporting data or independent verification procedures could lead to abuses by some providers. We are pleased that the PSHSB has been delegated the authority to order remedial action as needed on a case-by-case basis. However, the magnitude of the effort to review certifications and data from hundreds of service providers will be daunting.

- The FCC rules do not establish a procedure for interested or affected parties (i.e., state commissions or PSAPs) to challenge the reasonableness of a Covered 911 Service Provider certification that files using alternative measures.
- The FCC rules do not guarantee that state commissions (or PSAPs) will be able to obtain or access any protected confidential information supporting the Covered 911 Service Providers' annual certifications.
- The backup power requirements do not apply in Covered 911 Service Provider central offices that do not directly serve PSAPs or host a selective router. In the case of Verizon, the requirements would apply in only about a third of its total Virginia central offices.[37] This exclusion does not recognize that all offices (whether or not they directly serve a PSAP) are important in ensuring that customers can reach a PSAP at the time of an emergency. Of particular concern is excluding offices that host signal transport equipment that is necessary for 911 interoffice call completion.
- The FCC's rules do not encompass or address the circuits (lines) from end-users to the 911 selective router as well as the separate circuits required to enable

[37] We note that Verizon has backup power available in all its offices that meets or exceeds the FCC standards. This includes those offices that are not subject to the FCC's requirements since they do not house selective routers or directly serve PSAPs.

interoffice switching.[38] In other words, they do not address any potential problems affecting the customer's ability to dial or reach the PSAP from their side of the call.

Additional FCC Proceedings

On November 21, 2014, the FCC released a Policy Statement and Notice of Proposed Rulemaking in PS Docket Nos. 14-193 and 13-75 regarding the Matters of 911 Governance and Accountability and Improving 911 Reliability ("November 21, 2014 NPRM"). According to the November 21, 2014 NPRM, this proceeding is further evaluating the "the transition to Next Generation 911 (NG911) technologies to determine whether our rules should be revised or expanded to cover new best practices or additional entities...."[39] The FCC points out that recent "sunny day" 911 outages[40] demonstrate that there are public safety vulnerabilities that need to be addressed as the nation transitions to NG911. Accordingly, the FCC is proposing rules "designed to address failures leading to recent multi-state 911 outages, based on the October 2014 report of the Public Safety and Homeland Security Bureau."[41] [42]

The PSHSB 911 Outage Report focused on the April 9, 2014 outage which impacted more than 11 million people for up to six hours in seven states: California, Florida, Minnesota, North Carolina, Pennsylvania, South Carolina, and Washington (81

[38] Report and Order, para. 87. "Circuits from the end-user to the selective router lie beyond the scope of this proceeding."

[39] November 21, 2014 NPRM, para. 3.

[40] Outages that are not due to storms or disasters.

[41] November 21, 2014 NPRM, para. 4.

[42] On October 17, 2014, the PSHSB issued a Report and Recommendations in PS Docket No. 14-72 entitled "April 2014 Multistate 911 Outage: Cause and Impact." ("PSHSB 911 Outage Report").

141230097

PSAPs impacted). The PSHSB found that the outage was caused by a "preventable" software coding error in Intrado Inc.'s[43] 911 call routing facility in Englewood, Colorado.

On November 25, 2014, the FCC released a Notice of Proposed Rulemaking and Declaratory Ruling in PS Docket No. 14-174[44] and GN Docket No. 13-5[45] in which it is "seeking comment on modernizing its rules to ensure access to 911 service, protect consumers, and preserve competition" [46] as "the nation's communications networks are shifting from copper networks using legacy technologies to fiber, coaxial cable, and wireless networks using Internet Protocol (IP)-based technologies to carry voice, data and video."[47]

Among other matters, this NPRM will look at protecting consumers' ability to call 911 during a power outage on IP networks (non-copper lines). In particular, the release states the NPRM:

- Proposes a framework to establish reasonable expectations for when providers should bear responsibility for providing backup power solutions for the communications equipment at a customer's home during a power outage.
- Seeks comment on different backup power technologies and solutions in the marketplace today.
- Examines potential strategies for providing backup power during lengthy

---

[43] Intrado is a provider of 911 infrastructure and services to communications providers and to state and local PSAPs throughout the country.

[44] In the Matter of Ensuring Customer Premises Equipment Backup Power for Continuity of Communications.

[45] In the Matter of Technology Transitions.

[46] November 21, 2014 News Release issued by the FCC entitled "FCC Proposes Facilitating Technology Transitions by Modernizing Consumer Protection, Competition Rules."

[47] Ibid

power failures.

These two NPRMs do not address the operational deficiencies that were the root causes of the June 29 Derecho 911 outage[48] nor should they impact Verizon's corrective actions underway in Virginia. For the most part, Virginia PSAPs rely on legacy 911 services from Verizon (and other ILECs) as we have not yet transitioned to NG911 services in Virginia. These NPRMs highlight the additional challenges we may face in maintaining reliable 911 service as the legacy networks transition to an IP-based environment. We point out that many state commissions, including Virginia, may have limited or no jurisdiction over many of these IP technologies and service providers. This raises questions over if and how NG911 services will be regulated in the Commonwealth going forward. Of particular concern may be the transition period from legacy 911 systems to NG911.

RECOMMENDATIONS

From the start of our investigation, our goal has been to help prevent such a serious and life threatening event from occurring again. To that end, we are pleased with the progress Verizon has made in addressing and remediating the deficiencies and weaknesses found in its procedures, processes, and central offices. Nonetheless, in light of the critical public safety nature and importance of 911, we need to be cautious in modifying or eliminating the current requirements applied to Verizon in this proceeding. Furthermore, our evaluation of the FCC's new rules highlights some areas where we believe additional recommendations are warranted.

[48] As discussed earlier, those were addressed in the FCC's Report and Order.

Our revised recommendations[49] are as follows:

- Verizon should continue to correct all deficiencies and implement all recommendations identified in its 2012 and 2013 power audits conducted as required by this proceeding. The docket should remain open at least until all recommendations have been implemented.
- Verizon should provide the Staff with copies of any updates, revisions, or modifications to any of the initial 323 audits (including power, mechanical, and HVAC equipment) submitted in this proceeding.
- Verizon should continue to provide the Staff with quarterly corrective action progress reports on the actions taken as a result of items identified in the audits (including power, mechanical, and HVAC equipment) conducted as required in this proceeding. Upon request, Verizon should timely meet with the Staff to discuss such progress and other 911 related issues.
- Verizon should continue to provide a quarterly report to the Staff identifying any problems found in monthly testing of generators in Virginia offices. The report should identify the office and the corrective action undertaken and include applicable dates.
- Verizon should continue to meet and cooperate with PSAPs to ensure their concerns are addressed.
- The Staff should continue to meet and communicate with PSAPs and the 911 community.
- Verizon should provide the Staff with reasonable and timely access to monitor the

[49] These are intended to replace the recommendations set forth in our Final Report and the February 22, 2013 Order.

1462693

conditions in all Verizon central offices in Virginia.

- Verizon should provide the Staff with the Initial and Final Communications Outage Reports required pursuant to 47 C.F.R. Part 4 for outages impacting 911 service in Virginia. When providing such reports, Verizon should comply with all provisions of the FCC regulations related to report content, processing, and delivery. Upon request, Verizon should provide the Staff with additional information regarding a reported 911 service outage in Virginia that may not be included in the FCC report.
- Verizon should provide the Staff with copies of all applicable portions of the initial (October 15, 2015) and first full (October 15, 2016) annual certification reports filed with the FCC pursuant to 47 C.F.R. § 12.4, including any protected confidential information, that impact the reliability of 911 service (i.e., circuit auditing, backup power, and network monitoring) in Virginia.
- The Staff should continue to file an annual status report with the Commission that includes its recommendations.
- The Staff should continue to monitor and evaluate the FCC proceedings that impact the reliability and availability of 911 services in Virginia.

CONCLUSION

Verizon has made a concerted effort to identify and correct the underlying problems and failures leading to 911 outages following the June 29 Derecho. These changes should go a long way in preventing a similar outage in the future. Moreover, we strongly encourage Verizon to continue focusing on these efforts and most importantly to

1412260097

ensure its testing and maintenance is performed properly and timely in all its Virginia offices on an ongoing basis.

We are hopeful the certification rules adopted in the FCC Report and Order will provide the necessary incentive for Verizon and other LECs to comply with the necessary standards to ensure their emergency operational 911 readiness. It is too early to tell whether (or when) full compliance with the FCC's new rules will mitigate or replace the need for our continued oversight in this proceeding. Moreover, the many technological and statutory changes in the telecommunications marketplace (and their impact on 911) may warrant a need to revisit the Commission's current Rules Governing Enhanced 911 (E-911) Service (20VAC5-425).

Attachment 1

L-2012-097

1496521497

ELECTRONIC CODE OF FEDERAL REGULATIONS

e-CFR Data is current as of December 17, 2014

Title 47 → Chapter I → Subchapter A → Part 12 → §12.4

Title 47: Telecommunication
PART 12—RESILIENCY, REDUNDANCY AND RELIABILITY OF COMMUNICATIONS

---

§12.4 Reliability of covered 911 service providers.

(a) *Definitions.* Terms in this section shall have the following meanings:

(1) *Aggregation point.* A point at which network monitoring data for a 911 service area is collected and routed to a network operations center (NOC) or other location for monitoring and analyzing network status and performance.

(2) *Certification.* An attestation by a certifying official, under penalty of perjury, that a covered 911 service provider:

(i) Has satisfied the obligations of paragraph (c) of this section.

(ii) Has adequate internal controls to bring material information regarding network architecture, operations, and maintenance to the certifying official's attention.

(iii) Has made the certifying official aware of all material information reasonably necessary to complete the certification.

(iv) The term "certification" shall include both an annual reliability certification under paragraph (c) of this section and an initial reliability certification under paragraph (d)(1) of this section, to the extent provided under paragraph (d)(1) of this section.

(3) *Certifying official.* A corporate officer of a covered 911 service provider with supervisory and budgetary authority over network operations in all relevant service areas.

(4) *Covered 911 service provider.*

(i) Any entity that:

(A) Provides 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP), statewide default answering point, or appropriate local emergency authority as defined in §§64.3000(b) and 20.3 of this chapter; and/or

(B) Operates one or more central offices that directly serve a PSAP. For purposes of this section, a central office directly serves a PSAP if it hosts a selective router or ALI/ANI database, provides equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP.

(ii) The term "covered 911 service provider" shall not include any entity that:

(A) Constitutes a PSAP or governmental authority to the extent that it provides 911 capabilities; or

1452969

(B) Offers the capability to originate 911 calls where another service provider delivers those calls and associated number or location information to the appropriate PSAP.

(5) *Critical 911 circuits.* 911 facilities that originate at a selective router or its functional equivalent and terminate in the central office that serves the PSAP(s) to which the selective router or its functional equivalent delivers 911 calls, including all equipment in the serving central office necessary for the delivery of 911 calls to the PSAP(s). Critical 911 circuits also include ALI and ANI facilities that originate at the ALI or ANI database and terminate in the central office that serves the PSAP(s) to which the ALI or ANI databases deliver 911 caller information, including all equipment in the serving central office necessary for the delivery of such information to the PSAP(s).

(6) *Diversity audit.* A periodic analysis of the geographic routing of network components to determine whether they are physically diverse. Diversity audits may be performed through manual or automated means, or through a review of paper or electronic records, as long as they reflect whether critical 911 circuits are physically diverse.

(7) *Monitoring links.* Facilities that collect and transmit network monitoring data to a NOC or other location for monitoring and analyzing network status and performance.

(8) *Physically diverse.* Circuits or equivalent data paths are Physically Diverse if they provide more than one physical route between end points with no common points where a single failure at that point would cause both circuits to fail. Circuits that share a common segment such as a fiber-optic cable or circuit board are not Physically diverse even if they are logically diverse for purposes of transmitting data.

(9) *911 service area.* The metropolitan area or geographic region in which a covered 911 service provider operates a selective router or the functional equivalent to route 911 calls to the geographically appropriate PSAP.

(10) *Selective router.* A 911 network component that selects the appropriate destination PSAP for each 911 call based on the location of the caller.

(11) *Tagging.* An inventory management process whereby critical 911 circuits are labeled in circuit inventory databases to make it less likely that circuit rearrangements will compromise diversity. A covered 911 service provider may use any system it wishes to tag circuits so long as it tracks whether critical 911 circuits are physically diverse and identifies changes that would compromise such diversity.

(b) *Provision of reliable 911 service.* All covered 911 service providers shall take reasonable measures to provide reliable 911 service with respect to circuit diversity, central-office backup power, and diverse network monitoring. Performance of the elements of the certification set forth in paragraphs (c)(1)(i), (c)(2)(i), and (c)(3)(i) of this section shall be deemed to satisfy the requirements of this paragraph. If a covered 911 service provider cannot certify that it has performed a given element, the Commission may determine that such provider nevertheless satisfies the requirements of this paragraph based upon a showing in accordance with paragraph (c) of this section that it is taking alternative measures with respect to that element that are reasonably sufficient to mitigate the risk of failure, or that one or more certification elements are not applicable to its network.

(c) *Annual reliability certification.* One year after the initial reliability certification described in paragraph (d)(1) of this section and every year thereafter, a certifying official of every covered 911 service provider shall submit a certification to the Commission as follows.

(1) *Circuit auditing.*

(i) A covered 911 service provider shall certify whether it has, within the past year:

(A) Conducted diversity audits of critical 911 circuits or equivalent data paths to any PSAP served;

4412360697

(B) Tagged such critical 911 circuits to reduce the probability of inadvertent loss of diversity in the period between audits; and

(C) Eliminated all single points of failure in critical 911 circuits or equivalent data paths serving each PSAP.

(ii) If a covered 911 service provider does not conform with the elements in paragraph (c)(1)(i)(C) of this section with respect to the 911 service provided to one or more PSAPs, it must certify with respect to each such PSAP:

(A) Whether it has taken alternative measures to mitigate the risk of critical 911 circuits that are not physically diverse or is taking steps to remediate any issues that it has identified with respect to 911 service to the PSAP, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(2) *Backup power.*

(i) With respect to any central office it operates that directly serves a PSAP, a covered 911 service provider shall certify whether it:

(A) Provisions backup power through fixed generators, portable generators, batteries, fuel cells, or a combination of these or other such sources to maintain full-service functionality, including network monitoring capabilities, for at least 24 hours at full office load or, if the central office hosts a selective router, at least 72 hours at full office load; provided, however, that any such portable generators shall be readily available within the time it takes the batteries to drain, notwithstanding potential demand for such generators elsewhere in the service provider's network.

(B) Tests and maintains all backup power equipment in such central offices in accordance with the manufacturer's specifications;

(C) Designs backup generators in such central offices for fully automatic operation and for ease of manual operation, when required;

(D) Designs, installs, and maintains each generator in any central office that is served by more than one backup generator as a stand-alone unit that does not depend on the operation of another generator for proper functioning.

(ii) If a covered 911 service provider does not conform with all of the elements in paragraph (c)(2)(i) of this section, it must certify with respect to each such central office:

(A) Whether it has taken alternative measures to mitigate the risk of a loss of service in that office due to a loss of power or is taking steps to remediate any issues that it has identified with respect to backup power in that office, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(3) *Network monitoring.*

(i) A covered 911 service provider shall certify whether it has, within the past year:

14125097

(A) Conducted diversity audits of the aggregation points that it uses to gather network monitoring data in each 911 service area;

(B) Conducted diversity audits of monitoring links between aggregation points and NOCs for each 911 service area in which it operates; and

(C) Implemented physically diverse aggregation points for network monitoring data in each 911 service area and physically diverse monitoring links from such aggregation points to at least one NOC.

(ii) If a Covered 911 service provider does not conform with all of the elements in paragraph (c)(3)(i)(C) of this section, it must certify with respect to each such 911 service area:

(A) Whether it has taken alternative measures to mitigate the risk of network monitoring facilities that are not physically diverse or is taking steps to remediate any issues that it has identified with respect to diverse network monitoring in that 911 service area, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(d) *Other matters.*

(1) Initial reliability certification. One year after February 18, 2014, a certifying official of every covered 911 service provider shall certify to the Commission that it has made substantial progress toward meeting the standards of the annual reliability certification described in paragraph (c) of this section. Substantial progress in each element of the certification shall be defined as compliance with standards of the full certification in at least 50 percent of the covered 911 service provider's critical 911 circuits, central offices that directly serve PSAPs, and independently monitored 911 service areas.

(2) *Confidential treatment.*

(i) The fact of filing or not filing an annual reliability certification or initial reliability certification and the responses on the face of such certification forms shall not be treated as confidential.

(ii) Information submitted with or in addition to such certifications shall be presumed confidential to the extent that it consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements, information detailing specific corrective actions taken with respect to certification elements, or supplemental information requested by the Commission or Bureau with respect to a certification.

(3) *Record retention.* A covered 911 service provider shall retain records supporting the responses in a certification for two years from the date of such certification, and shall make such records available to the Commission upon request. To the extent that a covered 911 service provider maintains records in electronic format, records supporting a certification hereunder shall be maintained and supplied in an electronic format.

(i) With respect to diversity audits of critical 911 circuits, such records shall include, at a minimum, audit records separately addressing each such circuit, any internal report(s) generated as a result of such audits, records of actions taken pursuant to the audit results, and records regarding any alternative measures taken to mitigate the risk of critical 911 circuits that are not physically diverse.

(ii) With respect to backup power at central offices, such records shall include, at a minimum, records regarding the nature and extent of backup power at each central office that directly serves a PSAP, testing and maintenance records for backup power equipment in each such central office, and records regarding any alternative measures taken to mitigate the risk of insufficient backup power.

1460274097

(iii) With respect to network monitoring, such records shall include, at a minimum, records of diversity audits of monitoring links, any internal report(s) generated as a result of such audits, records of actions taken pursuant to the audit results, and records regarding any alternative measures taken to mitigate the risk of aggregation points and/or monitoring links that are not physically diverse.

[79 FR 3131, Jan. 17, 2014, as amended at 79 FR 7589, Feb. 10, 2014]

For questions or comments regarding e-CFR editorial content, features, or design, email ecfr@nara.gov.
For questions concerning e-CFR programming and delivery issues, email webteam@gpo.gov.